The Large Sieve and Its Applications (解析的整数論)

AUTHOR(S):

BOMBIERI, E.

数理解析研究所講究録
193巻 1973年 1-10

The large sieve and its applications

'oductory lecture on the recent developments in the theory
'e methods delivered on April 19,1973 at the Research Insti-
' the Mathematical Science of Kyoto University

By

Prof.Enrico Bombieri / Pisa University

;ext is noted and arranged by Y.Motohashi of Nihon University).

, Formulation of a sieve

$\mathcal{J}$ be the set of N integers n such that $M+1 \leq n \leq M+N$ where
ı arbitrary integer and N is an arbitrary positive integer. We
by $\mathcal{P}$ a set of prime numbers, and let Ω_p be some given set
idue classes mod p. We consider the sieve in which all integers
that $n \in \Omega_p$ for at least one prime number $p \in \mathcal{P}$ are deleted
. We denote this sieve by $(\mathcal{J}, \mathcal{P}, \Omega_p)$ and the set of unsifted
ts by $\mathcal{N}$, i.e.

$$\mathcal{N} = \{ n \in \mathcal{J} \mid n \notin \Omega_p , \forall p \in \mathcal{P} \}.$$

mple I. If we set

$$\mathcal{J} = \{ 1 \leq n \leq N \} , \quad \mathcal{P} = \{ p \leq \sqrt{N} \} , \quad \Omega_p = \{0\},$$

e have

$$\mathcal{N} = \{1\} \cup \{ \sqrt{N} < p \leq N \}.$$

mple II. If we set

$$\mathcal{I} = \{1 \le n \le N\}, \quad \mathcal{P} = \{p \le \sqrt{N}\}, \quad \Omega_2 =$$

$$\Omega_p = \{0, 2\} \quad (p \ge 3),$$

then $\mathcal{N}$ is the set of prime numbers $\sqrt{N} < p \le N$ such that p also a prime number. Thus this $\mathcal{N}$ is essentially the set primes not exceeding N.

Example III. If we set

$$\mathcal{I} = \{1 \le n \le N\}, \quad \mathcal{P} = \{\text{all prime numbers}\}$$

$$\Omega_p = \{\text{all quadratic non-residues mod } p\},$$

then $\mathcal{N}$ is the set of squares not exceeding N.

In the above examples I and II, $\mathcal{I}$ is sifted by only one residue classes mod p for each $p \in \mathcal{P}$, but in the last exam the cardinality of Ω_p, is $\frac{1}{2}(p-1)$ and so it can be very l In the first case, i.e. when $|\Omega_p|$ is very small on average, t nious method of Brun (later improved by Buchstab and Selber effective, but it looses its power as soon as we let $|\Omega_p|$ in indefinitely.

§2. The large sieve

In 1941 Linnik invented a quite ingenious method which en us to give an effective upper bound for the number of unsif elements in sieves for which $|\Omega_p|$ is large on average.

Let Z integers n_j satisfy

$$M < n_1 < n_2 < \ldots < n_z \le M+N. \tag{2}$$

We choose some number τ with $0 < \tau < 1$, and we call a prime p τ-exceptional if the number of residue classes mod p repre among the integers n_j is less than $(1-\tau)p$. Then Linnik pro

umber of τ-exceptional primes up to N is less than

$$CN/Z\tau^2 ,$$

s an absolute constant.

application, n_j should be considered to be unsifted
in the sieve such that $|\Omega_p| \geq \tau p$ and $p \in \mathcal{P}$, $p \leq \sqrt{N}$. Then the
) can be interpreted that

$$|\mathcal{N}| = Z \leq CN/|\mathcal{P}|\tau^2 .$$

y this is a quite good sieve-bound.

applied this "large sieve" to the very difficult problem
ogradov concerning the size of the least quadratic non-
odulo a prime. Vinogradov conjectured that the least quad-
-residue mod p is less than p^{ε}, where ε is an arbitrarily
itive constant. By the way, the hitherto best result is due
s who proved that the bound can be taken to be $p^{\frac{1}{4\sqrt{e}}+\varepsilon}$.
k proved that the number of prime numbers not exceeding x
the conjecture is false is less than the constant multiple
x. Linnik's proof runs as follows: Let n_j (j=1,..,Z) be
not exceeding N, which is composed entirely of prime divisors
r than N^{ε}. If the least quadratic non-residue mod p ($p \leq \sqrt{N}$)
than N^{ε}, then all n_j are obviously quadratic residue mod p.
an be considered to be $\frac{1}{2}$-exceptional for this sequence $\{n_j\}$,
ne result (3) the number of such primes does not exceed 4CN/Z.
s well known that N/Z is bounded by a constant which depends
. From this the result of Linnik follows at once.

§3. Rényi's version of the large sieve

Linnik's result (3) was generalized by Rényi, who applied it to the so-called Goldbach conjecture and made an extremely important contribution, namely he proved that every sufficiently large even integer is representable as a sum of an odd prime and a product of bounded number of prime numbers.

Developping his work Rényi found later the following formulation of the large sieve: Let $Z(p,a)$ denote the number of integers n_j of (2) such that $n_j \equiv a \bmod p$. Then if n_j is sufficiently dense in the interval $[M, M+N]$, it is expected that $Z(p,a)$ is near Z/p. Thus the variance

$$V(p) = \sum_{a=0}^{p-1} \left\{ Z(p,a) - \frac{Z}{p} \right\}^2$$

provides a measure of the regularity of distribution of n_j among the congruence classes mod p. And from the non-trivial estimation of the quantity

$$\sum_{p \in \mathcal{P}} p V(p) \tag{5}$$

we can deduce easily the consequence about the number of exceptional prime numbers. Thus the large sieve can be restated as the problem to find a good upper bound of (5).

In this way Rényi obtained

$$\sum_{p \le X} p V(p) \le 2NZ \tag{6}$$

for $X \le \left(\frac{N}{12}\right)^{\frac{1}{3}}$. But from the fact that Linnik's result (3) is effective even for $X \le \sqrt{N}$ we may expect the inequality (6) holds also for $X \le \sqrt{N}$. To this direction an important progress was made by Roth in

1964. Roth's method is similar in principle to that of Rényi, and he proved that Rényi's inequality (6),(apart from the particular constant 2 on the right), holds for

$$X = (N/\log N)^{\frac{1}{2}}.$$

Further important contribution was made by Bombieri in 1965, who proceeded along the line of Linnik and obtained

$$(7) \qquad \sum_{p \le X} p\nabla(p) \le 7(N+X^2)\log$$

for any X. This states that (6) holds for $X \le \sqrt{N}$, and thus the long standing conjecture is solved.

§4. Abstract formulation of the large sieve

It has been found recently that there is a strong connection between the large sieve and the Brun-Selberg sieve, and moreover another developments of the large sieve due to Halász, Montgomery and Gallagher have yielded striking results in the field of the density theorems for the zeros of Dirichlet's L-functions. Thus to give a common basis to these developments we state here an abstract version of the large sieve.

This is essentially a generalization of Bessel's inequality in a Hilbert space: Let $f, \varphi_1, \varphi_2, \ldots, \varphi_R$ be any elements of $\mathcal{H}$ a Hilbert space, then we have

$$(8) \qquad \sum_{j=1}^{R} |(f, \varphi_j)|^2 \left\{ \sum_{k=1}^{R} |(\varphi_j, \varphi_k)| \right\}^{-1} \le |f|^2.$$

If $\varphi_1, \ldots, \varphi_R$ are orthonomal elements of $\mathcal{H}$, then this reduces to the Bessel inequality. Similar inequalities has been found by Boas,Bellman, and Halász and Turán are the first who found its deep applications to the theory of Dirichlet's series. Bombieri found a

variation of the Bellman inequality and it was later refined to the above form by Selberg.

Now as an application to the large sieve itself, we take as $\mathcal{H}$ the linear space of square-summable sequences $\alpha=\{\alpha_n\}, -\infty<n<+\infty$, $\sum_{n=-\infty}^{+\infty}|\alpha_n|^2<+\infty$. The inner product is as usual

$$(\alpha,\beta)=\sum_{n=-\infty}^{+\infty}\alpha_n\overline{\beta_n}.$$

Further we pick up $f\in\mathcal{H}$ such that $f=\{a_n\}$

a_n : arbitrary complex numbers if $|n|\leq N$,

$a_n=0$ if $|n|>N$,

and in the above inequality (8) we take

$$\varphi_j=\begin{cases} e^{-2\pi i n x_j} & \text{if } |n|\leq N, \\ \left(\frac{N+L-|n|}{L}\right)^{\frac{1}{2}} e^{-2\pi i n x_j} & \text{if } N<|n|\leq N+L, \\ 0 & \text{if } |n|>N+L, \end{cases}$$

where L is a positive integer to be chosen appropriately. Then we have the following result : Let $x_1,\ldots,x_R$ be an arbitrary set of real numbers, and we suppose that there is a positive number $(0<\delta<1)$ such that

$$|x_i-x_j|>\delta \pmod 1$$

for any $i\neq j$. Let $S(x)$ be the trigonometrical polynomial

$$S(x)=\sum_{1\leq n\leq N}a_n e^{2\pi i n x}.$$

Then we have

$$\sum_{j=1}^{R}|S(x_j)|^2\leq(N+2\delta^{-1})\sum_{1\leq n\leq N}|a_n|^2. \tag{9}$$

In this result we set $a_n=0$ or 1 and x_j the rational point with denominator $\leq Q$. Then we find

$$(10) \qquad \sum_{q \le Q} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \left| S\left(\frac{a}{q}\right) \right|^2 \le (N + 2Q^2) Z,$$

where

$$Z = \sum_{\substack{1 \le n \le N \\ a_n = 1}} 1$$

This inequality is an improvement of (7), since it is easy to see that for any prime p

$$p\, V(p) = \sum_{a=1}^{p-1} \left| S\left(\frac{a}{p}\right) \right|^2.$$

But the above inequality contains the sum over not only prime numbers but also composit numbers, and if we consider the contribution of composit numbers, we can deduce a result similar to the Brun-Selberg sieve. This has been realized firstly by Bombieri and Davenport. And their proof has been elaborated by Montgomery who proved through (10) that

$$|\mathcal{N}| \le \frac{N + 2Q^2}{\sum_{q \le Q} \mu^2(q) \prod_{p \mid q} \frac{|\Omega_p|}{p - |\Omega_p|}},$$

where $\mathcal{N}$ is defined by (1) and $\mu(q)$ is the Möbius function. This is completely similar to the main term which appears in the Selberg sieve, but its real advantage is that it holds regardless of the size of $|\Omega_p|$.

§5. Hybrid large moduli theorems

As is already mentioned, the inequality (8) contains both the large sieve and the device of Halász. But recently Halász' device got much improvements by Montgomery and Gallagher, and so here we

try to give an abstract formulation of their methods.

Let Ω denote a finite set of multiplicative characters $\omega(n) = \chi(n)n^{it}$, where χ is a Dirichlet character and t is an arbitrary real number. And let $\{a_n\}_{n\leq N}$ be an arbitrary finite sequence of complex numbers. Then the correspondence

$$\mathscr{D} : \{a_n\} \longrightarrow \sum_{n\leq N} a_n \omega(n)$$

can be considered to be an operator (an $N \times |\Omega|$-matrix) which maps $L^2(\mathscr{N})$ to $L^2(\Omega)$, where $\mathscr{N}$ is the set of positive integers $\leq N$. As is well known, if $\mathscr{D}^*$ is the adjoint operator of $\mathscr{D}$, then the maximum eigenvalue of $\mathscr{D}\mathscr{D}^*$ coincides with that of $\mathscr{D}^*\mathscr{D}$. Thus to estimate K of the inequality, which holds for all $\{a_n\}$,

$$\sum_{\omega\in\Omega} \Big| \sum_{n\leq N} a_n \omega(n) \Big|^2 \leq K \sum_{n\leq N} |a_n|^2,$$

it is sufficient to find a good upper bound of $\tilde{K}$ of the inequality

$$\sum_{n\leq N} \Big| \sum_{\omega} \alpha_\omega \bar{\omega}(n) \Big|^2 \leq \tilde{K} \sum_{\omega\in\Omega} |\alpha_\omega|^2 \tag{11}$$

which should also hold for any $\{\alpha_\omega\}$. Now to do this we introduce a function f(x) such that

$$f(n) \geq 1 \text{ for } n \leq N,$$

$$f(n) \geq 0 \text{ for } n > N.$$

Then we see the left side of (11) is not larger than

$$\sum_{n=1}^{\infty} f(n) \Big| \sum_{\omega\in\Omega} \alpha_\omega \bar{\omega}(n) \Big|^2$$

$$= \sum_{\omega,\omega'\in\Omega} \alpha_\omega \bar{\alpha}_{\omega'} \sum_{n=1}^{\infty} f(n)\bar{\omega}\omega'(n).$$

And so we have to estimate the inner sum over positive integers. We put (for example)

$$f(n) = \left(\frac{n}{N}\right)^{-\sigma} e^{-\left(\frac{n}{N}\right)^k},$$

where σ, k are arbitrary positive numbers to be chosen appropriately. Then we have, since $\omega(n) = \chi(n)n^{it}$, $\omega'(n) = \chi'(n)n^{it'}$,

$$\sum_{n=1}^{\infty} f(n)\bar{\omega}\omega'(n)$$

$$= N^{\sigma} \sum_{n=1}^{\infty} e^{-(\frac{n}{N})^k} \bar{\chi}\chi'(n) n^{-\sigma - i(t-t')}$$

$$= \frac{N^{\sigma}}{2\pi i} \int_{(\mathrm{Re}\, w > 1-\sigma)} L(\sigma + i(\tau - t') + w, \bar{\chi}\chi') \Gamma(\frac{w}{k} + 1) \frac{N^w}{w} dw,$$

where $L(s,\chi)$ is the Dirichlet L-function attached to the character χ, and $\Gamma(w)$ is the usual gamma function. Here we introduce the concept of "well-spacedness" to the set Ω : We say that Ω is well spaced, if for any $\omega \neq \omega'$ ($\omega, \omega' \in \Omega$) we have either that $\bar{\chi}\chi'$ is non-principal mod q or that $|t - t'| > (\log D)^2$, where D is defined by

$$D = (\max |t| + 1)(\max q).$$

Then by the known estimate of $L(s,\chi)$ we can conclude that

(12) $$K \ll (N + D) (\log DN)^c$$

or

(13) $$K \ll (N + D^{\frac{1}{2}}|\Omega|)(\log DN)^c,$$

where c is an absolute constant.

(12) corresponds to the hybrid mean value theorem of Gallagher and Montgomery, and (13) to the improved form due to Montgomery of Halász' device.

Finally we state some deep applications of (12) and (13) to the theory of Riemann's zeta-function $\zeta(s)$ and Dirichlet's L-functions

$L(s,\chi)$ $(s=\sigma+it)$.

Let $N(\alpha,T)$ and $N(\alpha,T,\chi)$ denote the number of zeros of $\zeta(s)$ and $L(s,\chi)$, respectively, in the rectangle

$$\alpha \leq \sigma \leq 1 , \quad |t| \leq T$$

Then from (12) we get

$$N(\alpha, T) \ll T^{3\frac{1-\alpha}{2-\alpha}} \log^c T,$$

and from (13)

$$N(\alpha, T) \ll T^{\frac{12}{5}(1-\alpha)} \log^c T.$$

The first is the classical result of Ingham, and the second is the hitherto best result due to Huxley, from which we can deduce that $p_{n+1} - p_n \leq p_n^{\frac{7}{12}+\varepsilon}$, where p_n denotes the n-th prime number. The application itself of (12) and (13) is not actually difficult, but the real difficulty is the construction of Dirichlet polynomials which takes large value at the zeros of $\zeta(s)$ or $L(s,\chi)$. In this respect the following result of Gallagher, which is an extension of results due to Linnik and Fogels and is an application of an improved form of (12), is a typical one:

$$\sum_{q \leq T} \sum_{\chi \bmod q}^{*} N(\alpha, T, \chi) \ll T^{c_0(1-\alpha)},$$

where $\sum^{*}$ denotes a sum over all primitive characters mod q and c_0 is an absolute constant.